116TH CONGRESS
1ST SESSION

H. R. 328

To require the Secretary of State to design and establish a Vulnerability Disclosure Process (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 8, 2019

Mr. TED LIEU of California (for himself and Mr. YOHO) introduced the following bill; which was referred to the Committee on Foreign Affairs

A BILL

To require the Secretary of State to design and establish a Vulnerability Disclosure Process (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ‘‘Hack Your State Department Act’’.

SEC. 2. DEFINITIONS.

In this Act:

(1) BUG BOUNTY PROGRAM.—The term ''bug bounty program'' means a program under which an approved individual, organization, or company is temporarily authorized to identify and report vulnerabilities of internet-facing information technology of the Department in exchange for compensation.

(2) DEPARTMENT.—The term ''Department'' means the Department of State.

(3) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given such term in section 11101 of title 40, United States Code.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of State.

SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLOSURE PROCESS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall design, establish, and make publicly known a Vulnerability Disclosure Process (VDP) to improve Department cybersecurity by—

(1) providing security researchers with clear guidelines for—

(A) conducting vulnerability discovery activities directed at Department information technology; and

(B) submitting discovered security vulnerabilities to the Department; and

(2) creating Department procedures and infrastructure to receive and fix discovered vulnerabilities.

(b) REQUIREMENTS.—In establishing the VDP pursuant to paragraph (1), the Secretary shall—

(1) identify which Department information technology should be included in the process;

(2) determine whether the process should differentiate among and specify the types of security vulnerabilities that may be targeted;

(3) provide a readily available means of reporting discovered security vulnerabilities and the form in which such vulnerabilities should be reported;

(4) identify which Department offices and positions will be responsible for receiving, prioritizing, and addressing security vulnerability disclosure reports;

(5) consult with the Attorney General regarding how to ensure that individuals, organizations, and companies that comply with the requirements of the

process are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for specific activities authorized under the process;

(6) consult with the relevant offices at the Department of Defense that were responsible for launching the 2016 Vulnerability Disclosure Program, ''Hack the Pentagon'', and subsequent Department of Defense bug bounty programs;

(7) engage qualified interested persons, including nongovernmental sector representatives, about the structure of the process as constructive and to the extent practicable; and

(8) award contracts to entities, as necessary, to manage the process and implement the remediation of discovered security vulnerabilities.

(c) ANNUAL REPORTS.—Not later than 180 days after the establishment of the VDP under subsection (a) and annually thereafter for the next six years, the Secretary of State shall submit to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate a report on the VDP, including information relating to the following:

(1) The number and severity, in accordance with the National Vulnerabilities Database of the

National Institute of Standards and Technology, of security vulnerabilities reported.

(2) The number of previously unidentified security vulnerabilities remediated as a result.

(3) The current number of outstanding previously unidentified security vulnerabilities and Department of State remediation plans.

(4) The average length of time between the reporting of security vulnerabilities and remediation of such vulnerabilities.

(5) The resources, surge staffing, roles, and responsibilities within the Department used to implement the VDP and complete security vulnerability remediation.

(6) Any other information the Secretary determines relevant.

SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PROGRAM.

(a) ESTABLISHMENT OF PILOT PROGRAM.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary shall establish a bug bounty pilot program to minimize security vulnerabilities of internet-facing information technology of the Department.

(2) REQUIREMENTS.—In establishing the pilot program described in paragraph (1), the Secretary shall—

(A) provide compensation for reports of previously unidentified security vulnerabilities within the websites, applications, and other internet-facing information technology of the Department that are accessible to the public;

(B) award contracts to entities, as necessary, to manage such pilot program and for executing the remediation of security vulnerabilities identified pursuant to subparagraph (A);

(C) identify which Department information technology should be included in such pilot program;

(D) consult with the Attorney General on how to ensure that individuals, organizations, or companies that comply with the requirements of such pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law for specific activities authorized under such pilot program;

(E) consult with the relevant offices at the Department of Defense that were responsible for launching the 2016 ''Hack the Pentagon'' pilot program and subsequent Department of Defense bug bounty programs;

(F) develop a process by which an approved individual, organization, or company can register with the entity referred to in subparagraph (B), submit to a background check as determined by the Department, and receive a determination as to eligibility for participation in such pilot program;

(G) engage qualified interested persons, including nongovernmental sector representatives, about the structure of such pilot program as constructive and to the extent practicable; and

(H) consult with relevant United States Government officials to ensure that such pilot program complements persistent network and vulnerability scans of the Department of State's internet-accessible systems, such as the scans conducted pursuant to Binding Operational Directive BOD–15–01.

(3) DURATION.—The pilot program established under paragraph (1) should be short-term in duration and not last longer than one year.

(b) REPORT.—Not later than 180 days after the date on which the bug bounty pilot program under subsection (a) is completed, the Secretary shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report on such pilot program, including information relating to—

(1) the number of approved individuals, organizations, or companies involved in such pilot program, broken down by the number of approved individuals, organizations, or companies that—

(A) registered;

(B) were approved;

(C) submitted security vulnerabilities; and

(D) received compensation;

(2) the number and severity, in accordance with the National Vulnerabilities Database of the National Institute of Standards and Technology, of security vulnerabilities reported as part of such pilot program;

(3) the number of previously unidentified security vulnerabilities remediated as a result of such pilot program;

(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

(5) the average length of time between the reporting of security vulnerabilities and remediation of such vulnerabilities;

(6) the types of compensation provided under such pilot program; and

(7) the lessons learned from such pilot program.

○